

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-250193

(43)Date of publication of application : 17.09.1999

(51)Int.Cl.

G06K 17/00

G06F 19/00

G07G 1/12

(21)Application number : 10-052133

(71)Applicant : OKI ELECTRIC IND CO LTD

(22)Date of filing : 04.03.1998

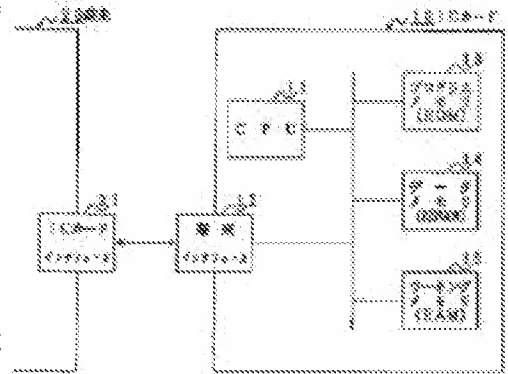
(72)Inventor : KAMIMURA AKITOSHI

(54) IC CARD AND ITS TRANSACTION PROCESSING METHOD

(57)Abstract:

PROBLEM TO BE SOLVED: To prevent the illegal use of an IC card and the illegal drawing of electronic money by setting a flag without fail before unlocking, releasing the flag after setting locking and setting locking in a case when the flag is previously set.

SOLUTION: The IC card 10 compares a password sent from a customer and a password previously registered in a data memory 14 and when the passwords are coincident with each other, the flag setting means of CPU 11 sets the flag 1 in the memory 14 by setting or clearing. Continually, the IC card 10 unlocks the locking by the unlocking means of CPU 11. Then, after unlocking, the IC card 10 executes prescribed processing by the processing means of CPU 11. Continually, after setting locking by the locking setting means of CPU 11, the IC card 10 releases the flag 1 by clearing or setting by the flag releasing means of CPU 11.



(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平11-250193

(43) 公開日 平成11年(1999) 9月17日

(51) Int.Cl. ⁶	識別記号	F I	
G 0 6 K 17/00		C 0 6 K 17/00	B
			L
			S
G 0 6 F 19/00		C 0 7 G 1/12	3 2 1 P
G 0 7 G 1/12	3 2 1	C 0 6 F 15/30	3 5 0

審査請求 未請求 請求項の数 4 O L (全 7 頁)

(21) 出願番号 特願平10-52133

(22) 出願日 平成10年(1998) 3月4日

(71) 出願人 000000295

沖電気工業株式会社

東京都港区虎ノ門1丁目7番12号

(72) 発明者 上村 明利

東京都港区虎ノ門1丁目7番12号 沖電気
工業株式会社内

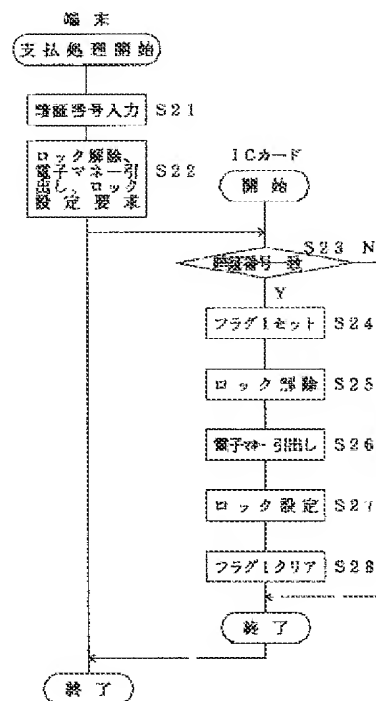
(74) 代理人 弁理士 川合 誠 (外1名)

(54) 【発明の名称】 ICカード及びその取引処理方法

(57) 【要約】

【課題】 ICカードが不正に使用されることがなく、電子マネーが不正に引き出されることがないようにする。

【解決手段】 端末からコマンドが送られたときに、内部に形成されたフラグを設定するフラグ設定手段と、フラグが設定された状態でロックを解除するロック解除手段と、ロックが解除された状態で所定の処理を行う処理手段と、処理が終了した後にロックを設定する第1のロック設定手段と、ロックが設定された後に前記フラグを解除するフラグ解除手段と、あらかじめフラグが設定されている場合に、ロックを設定する第2のロック設定手段とを有する。ロックを解除する前に、フラグが必ず設定され、ロックが設定された後にフラグが解除されるとともに、あらかじめフラグが設定されている場合に、ロックが設定される。



【特許請求の範囲】

【請求項1】 (a) 端末からコマンドが送られたときに、内部に形成されたフラグを設定するフラグ設定手段と、(b) 前記フラグが設定された状態でロックを解除するロック解除手段と、(c) 前記ロックが解除された状態で所定の処理を行う処理手段と、(d) 前記処理が終了した後にロックを設定する第1のロック設定手段と、(e) 前記ロックが設定された後に前記フラグを解除するフラグ解除手段と、(f) あらかじめフラグが設定されている場合に、ロックを設定する第2のロック設定手段とを有することを特徴とするICカード。

【請求項2】 前記端末からの一つのコマンドに基づいて、前記ロック解除手段によるロックの解除、前記処理手段による所定の処理、及び前記第1のロック設定手段によるロックの設定が、一連の動作で排他的に行われる請求項1に記載のICカード。

【請求項3】 前記処理手段は、あらかじめ設定された動作可能条件が満たされたときに前記処理を行う請求項1に記載のICカード。

【請求項4】 (a) 端末からICカードにコマンドが送られたときに、ICカードの内部に形成されたフラグを設定し、(b) フラグが設定された状態でICカードのロックを解除し、(c) ロックが解除された状態で所定の処理を行い、(d) 処理が終了した後にICカードのロックを設定し、(e) 該ロックが設定された後に前記フラグを解除するとともに、(f) あらかじめ前記フラグが設定されている場合に、ICカードにロックを設定することを特徴とするICカードの取引処理方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、ICカード及びその取引処理方法に関するものである。

【0002】

【従来の技術】従来、電子マネーが充填（てん）されたICカードは、商店等においてプリペイド方式又はポストペイド方式で使用されるようになっていた。その場合、例えば、商店に設置された電子マネー用の端末の挿入・引出口に顧客又は店員がICカードを差し込み、店員が前記端末を操作して支払額を入力すると、端末の表示部に支払額が表示されるようになっていた。

【0003】そして、店員が顧客に対して支払額の確認を求め、顧客が例えば、「YES」キーを押すと、端末とICカードとの間において取引処理としての支払処理が開始され、支払額に相当する分の電子マネーがICカードから引き出され、端末に入金される。続いて、前記表示部に支払処理が終了したことが表示されると、顧客又は店員はICカードを端末の挿入・引出口から引き抜く。

【0004】次に、前記ICカードの支払処理について説明する。図2は従来のICカードの支払処理方法を示

すフローチャートである。まず、端末がICカードにコマンドを送り、ICカードのロック状態を問い合わせると、該ICカードはロック状態を端末に回答する。このとき、端末は前記ICカードからの回答に基づいて、ICカードにおいてロックが設定されているかどうかを判断する。

【0005】ところで、ICカードにおいてロックが設定されている場合、電子マネーを引き出すことはできない。そこで、前記端末は、ロックが設定されている旨を表示部に表示し、顧客にロックを解除するための暗証番号を入力するよう促す。これに対して顧客が暗証番号を入力すると、端末は、ICカードに暗証番号を送り、ロックを解除するよう要求する。

【0006】続いて、ICカードは、送られた暗証番号と内蔵するデータメモリにあらかじめ登録された暗証番号とを比較し、両暗証番号が一致すると、ロックを解除する。次に、端末は、ICカードに引出額を送り、ICカード内の電子マネーの引出しを要求する。そして、ICカードは要求された電子マネーを引き出し、端末に入金する。このようにして、ICカードから電子マネーが引き出されると、端末はICカードにロックを設定するよう要求し、該ICカードは端末からの要求に従ってロックを設定する。

【0007】なお、ICカードにおいてロックが設定されていない場合、端末は、ICカードに引出額を送り、ICカード内の電子マネーの引出しを要求する。そして、ICカードは要求された電子マネーを引き出し、端末に入金する。次に、フローチャートについて説明する。

ステップS1 端末はICカードのロック状態を問い合わせる。

ステップS2 ICカードはロック状態を端末に回答する。

ステップS3 端末はICカードにおいてロックが設定されているかどうかを判断する。ロックが設定されている場合はステップS4に、ロックが設定されていない場合はステップS8に進む。

ステップS4 暗証番号を入力する。

ステップS5 端末はICカードにロックを解除するよう要求する。

ステップS6 ICカードは、送られた暗証番号とデータメモリにあらかじめ登録された暗証番号とが一致するかどうかを判断する。暗証番号が一致した場合はステップS7に進み、一致しない場合は処理を終了する。

ステップS7 ICカードはロックを解除する。

ステップS8 端末はICカード内の電子マネーの引出しを要求する。

ステップS9 ICカードは要求された電子マネーを引き出す。

ステップS10 端末はICカードにロックを設定する

よう要求する。

ステップS11 ICカードはロックを設定する。

【0008】

【発明が解決しようとする課題】しかしながら、前記従来のICカードにおいては、支払処理中にロックが解除された状態でICカードが奪取された場合等にICカードが不正に使用されると、電子マネーが不正に引き出されてしまう。本発明は、前記従来のICカードの問題点を解決して、ICカードが不正に使用されることがなく、電子マネーが不正に引き出されることがないICカード及びその取引処理方法を提供することを目的とする。

【0009】

【課題を解決するための手段】そのために、本発明のICカードにおいては、端末からコマンドが送られたときに、内部に形成されたフラグを設定するフラグ設定手段と、前記フラグが設定された状態でロックを解除するロック解除手段と、前記ロックが解除された状態で所定の処理を行う処理手段と、前記処理が終了した後にロックを設定する第1のロック設定手段と、前記ロックが設定された後に前記フラグを解除するフラグ解除手段と、あらかじめフラグが設定されている場合に、ロックを設定する第2のロック設定手段とを有する。

【0010】本発明のICカードの取引処理方法においては、端末からICカードにコマンドが送られたときに、ICカードの内部に形成されたフラグを設定し、フラグが設定された状態でICカードのロックを解除し、ロックが解除された状態で所定の処理を行い、処理が終了した後にICカードのロックを設定し、該ロックが設定された後に前記フラグを解除する。

【0011】そして、あらかじめ前記フラグが設定されている場合に、ICカードにロックを設定する。

【0012】

【発明の実施の形態】以下、本発明の実施の形態について図面を参照しながら詳細に説明する。図3は本発明の第1の実施の形態におけるICカードの取引処理装置を示すブロック図である。図において、10はICカード、11は該ICカード10の制御を行うCPU、12は端末20とのインタフェースを行う端末インタフェース、13は制御プログラムを格納するプログラムメモリ（ROM）、14はデータが格納されるデータ不揮発性のデータメモリ（EEPROM）、15は前記ICカード10を動作させるためのワーキングメモリ（RAM）、21は前記ICカード10とのインタフェースを行うICカードインタフェースである。なお、ICカード10及び端末20によって取引処理装置が構成される。

【0013】次に、前記ICカード10の取引処理としての支払処理について説明する。図1は本発明の第1の実施の形態におけるICカードの支払処理方法を示すフ

ローチャートである。まず、端末20（図3）は、所定の表示を図示されない表示部に行い、顧客にロックを解除するための暗証番号を入力するよう促す。これに対して顧客が暗証番号を入力すると、端末20は、ICカード10に暗証番号を送り、所定の一つのコマンドによって、ロックを解除するよう要求するとともに、ICカード10に引出額を送り、ICカード10内の電子マネーの引出し、及びロックの設定を要求する。

【0014】続いて、ICカード10は、送られた暗証番号と前記データメモリ14にあらかじめ登録された暗証番号とを比較し、両暗証番号が一致すると、CPU11の図示されないフラグ設定手段により、データメモリ14内のフラグ1をセット又はクリアすることによって設定する。なお、本実施の形態においては、前記フラグ設定手段はフラグ1をセットする。続いて、前記ICカード10は、CPU11の図示されないロック解除手段によってロックを解除する。

【0015】なお、両暗証番号が一致しない場合、ICカード10は前記各要求を拒否して支払処理を終了する。そして、ICカード10は、ロックを解除した後、CPU11の図示されない処理手段によって所定の処理を行う。なお、本実施の形態において、前記処理手段は、要求された電子マネーを引き出す。続いて、ICカード10は、CPU11の図示されない第1のロック設定手段によってロックを設定した後、CPU11の図示されないフラグ解除手段により、前記フラグ1をクリア又はセットすることによって解除する。なお、本実施の形態において、前記フラグ解除手段は、前記フラグ1をクリアする。

【0016】次に、フローチャートについて説明する。ステップS21 暗証番号を入力する。

ステップS22 端末20は、ICカード10に暗証番号を送り、ロックの解除、電子マネーの引出し、及びロックの設定を要求する。

ステップS23 ICカード10は、送られた暗証番号とデータメモリ14にあらかじめ登録された暗証番号とが一致するかどうかを判断する。暗証番号が一致した場合はステップS24に進み、一致しない場合は処理を終了する。

ステップS24 フラグ1をセットする。

ステップS25 ICカード10はロックを解除する。

ステップS26 ICカード10は要求された電子マネーを引き出す。

ステップS27 ICカード10はロックを設定する。

ステップS28 フラグ1をクリアする。

【0017】次に、ICカード10の初期化動作について説明する。図4は本発明の第1の実施の形態におけるICカードの初期化動作を示すフローチャートである。まず、ICカード10（図3）は、データメモリ14内のフラグ1をチェックし、フラグ1がセットされている

かどうかを判断する。そして、ICカード10は、前記フラグ1がクリアされている場合は、そのまま初期化動作を継続し、フラグ1がセットされている場合は、CPU11の図示されない第2のロック設定手段によってロックを設定した後、前記フラグ1をクリアし、そのまま初期化動作を継続する。

【0018】次に、フローチャートについて説明する。ステップS31 フラグ1がセットされているかどうかを判断する。フラグ1がセットされている場合はステップS32に、フラグ1がクリアされている場合はステップS34に進む。

ステップS32 ロックを設定する。

ステップS33 フラグ1をクリアする。

ステップS34 初期化動作を継続する。

【0019】このように、本実施の形態においては、一つのコマンドがICカード10に送られるだけで、ICカード10は、ロックの解除、電子マネーの引出し、及びロックの設定から成る一連の動作を排他的に行うようになっているので、その間にICカード10に他のコマンドを送るのが困難になる。したがって、ロックが解除された状態でICカード10が不正に使用されることがなくなり、電子マネーが不正に引き出されることがない。

【0020】また、ICカード10において、ロックを解除する前にフラグ1が必ずセットされ、ロックが設定された後にフラグ1がクリアされるとともに、初期化動作時において、ICカード10は、フラグ1をチェックし、フラグ1がセットされている場合、ロックを設定するようになっているので、支払処理中にロックが解除された状態でICカード10が奪取された場合、ICカードを不正に使用しようとしても、フラグ1がセットされているので、初期化動作時においてICカード10が自らロックを設定することになる。したがって、ICカード10が不正に使用されることがなく、電子マネーが不正に引き出されることがない。

【0021】なお、本実施の形態においては、一つのコマンドに基づいて、ロックの解除、電子マネーの引出し、及びロックの設定から成る一連の動作が排他的に行われるようになっているが、ロックの解除、電子マネーの引出し、及びロックの設定の各動作を別々のコマンドに基づいて行うこともできる。また、ICカード10は、初期化動作時にフラグ1をチェックし、該フラグ1がセットされている場合にロックを設定するようになっているが、端末20からコマンドが送られたときに、コマンドを実行する前に前記フラグ1をチェックし、該フラグ1がセットされている場合にロックを設定することもできる。

【0022】次に、本発明の第2の実施の形態について説明する。なお、第1の実施の形態と同じ構造を有するものについては、同じ符号を付与することによってその

説明を省略する。図5は本発明の第2の実施の形態におけるICカードの支払処理方法を示す第1のフローチャート、図6は本発明の第2の実施の形態におけるICカードの支払処理方法を示す第2のフローチャートである。

【0023】まず、端末20（図3）は、所定の表示を図示されない表示部に行い、顧客にロックを解除するための暗証番号を入力するよう促す。これに対して顧客が暗証番号を入力すると、端末20は、ICカード10に暗証番号を送り、所定のコマンドによって、ロックを解除するよう要求する。このとき、端末20は、例えば、引出回数の最大値を1回に、引出金額の最大値を今回の引出額に設定してICカード10に送る。なお、本実施の形態においては、前記引出回数及び引出金額の各最大値によって動作可能条件が構成される。

【0024】次に、ICカード10は、送られた暗証番号と前記データメモリ14にあらかじめ登録された暗証番号とを比較し、両暗証番号が一致すると、CPU11の図示されないフラグ設定手段により、データメモリ14内のフラグ2をセット又はクリアすることによって設定するとともに、端末20から送られた引出回数及び引出金額の各最大値をデータメモリ14に設定し、続いて、CPU11の図示されないロック解除手段によってロックを解除する。なお、本実施の形態においては、前記フラグ設定手段はフラグ2をセットする。

【0025】また、両暗証番号が一致しない場合、ICカード10はロックを解除する旨の要求を拒否して支払処理を終了する。次に、端末20は、ICカード10に引出額を送り、ICカード10内の電子マネーの引出しを要求する。これに対して、ICカード10は、フラグ2をチェックし、フラグ2がセットされている場合は、前記引出回数及び引出金額の各最大値をチェックして前記動作可能条件が満たされているかどうかを判断する。そして、前記動作可能条件が満たされている場合、すなわち、引出回数の最大値が0より大きく、引出金額が最大値以下である場合、引出回数及び引出金額の各最大値を更新し、引出回数の最大値を1だけ減算し、引出金額の最大値を今回の引出金額分だけ減算した後、CPU11の図示されない処理手段によって所定の処理を行う。なお、本実施の形態において、前記処理手段は、要求された電子マネーを引き出す。

【0026】そして、前記フラグ2がクリアされている場合は、要求された電子マネーを引き出す。さらに、前記動作可能条件が満たされていない場合、すなわち、引出回数が0であり、引出金額が最大値より大きい場合は、引出エラーを応答する。そして、ICカード10から正常に電子マネーを引き出すことができると、端末20は、ICカード10にロックを設定するよう要求する。続いて、ICカード10は、CPU11の図示されない第1のロック設定手段によってロックを設定した

後、CPU11の図示されないフラグ解除手段により、前記フラグ2をクリア又はセットすることによって解除する。なお、本実施の形態において、前記フラグ解除手段は、前記フラグ2をクリアする。

【0027】次に、フローチャートについて説明する。

ステップS41 暗証番号を入力する。

ステップS42 端末20はICカード10にロックを解除するよう要求する。

ステップS43 ICカード10は、送られた暗証番号とデータメモリ14にあらかじめ登録された暗証番号とが一致するかどうかを判断する。暗証番号が一致した場合はステップS44に進み、一致しない場合は処理を終了する。

ステップS44 フラグ2をセットし、引出回数及び引出金額の最大値を設定する。

ステップS45 ICカード10はロックを解除する。

ステップS46 端末20はICカード10に電子マネーを引き出すよう要求する。

ステップS47 ICカード10はフラグ2をチェックし、フラグ2がセットされているかどうかを判断する。フラグ2がセットされている場合はステップS48に、フラグ2がセットされていない場合はステップS50に進む。

ステップS48 ICカード10は引出回数の最大値が0より大きく、引出金額が最大値以下であるかどうかを判断する。引出回数の最大値が0より大きく、引出金額が最大値以下である場合はステップS49に、そうでない場合はステップS51に進む。

ステップS49 ICカード10は引出回数及び引出金額の最大値を更新し、引出回数の最大値を1だけ減算し、引出金額の最大値を今回の引出金額分だけ減算する。

ステップS50 ICカード10は要求された電子マネーを引き出す。

ステップS51 引出エラーを応答する。

ステップS52 端末20はICカード10にロックを設定するよう要求する。

ステップS53 ICカード10はロックを設定する。

ステップS54 フラグ2をクリアする。

【0028】このように、本実施の形態においては、ICカード10において、ロックを解除する前に引出回数及び引出金額の最大値が設定されるとともに、電子マネーの引出しに伴って最大値が更新される。したがって、支払処理中にロックが解除された状態でICカード10が奪取された場合、ICカードを不正に使用しようとしても、引出回数が0になるか、引出金額が最大値より大きくなると、電子マネーの引出しの要求が拒否されるので、ICカード10が不正に使用されることがなく、電子マネーが不正に引き出されることがない。

【0029】なお、ICカード10は、ロックの解除が

要求されると、引出回数の最大値を1回に、引出金額の最大値を今回の引出額に設定するようになっているが、端末20において別のコマンドを発生させ、該コマンドによって任意の引出回数の最大値及び引出金額の最大値の原本をICカード10に送ることもできる。その場合、ICカード10は、前記最大値の原本をデータメモリ14に格納し、ロックを解除するときに、データメモリ14に格納された最大値の原本をチェック用の領域にコピーし、コピーされた最大値の原本を利用することもできる。

【0030】前記各実施の形態においては、電子マネーが充填されたICカードについて説明しているが、他のICカードに適用することもできる。なお、本発明は前記実施の形態に限定されるものではなく、本発明の趣旨に基づいて種々変形させることが可能であり、それらを本発明の範囲から排除するものではない。

【0031】

【発明の効果】以上詳細に説明したように、本発明によれば、ICカードにおいては、端末からコマンドが送られたときに、内部に形成されたフラグを設定するフラグ設定手段と、前記フラグが設定された状態でロックを解除するロック解除手段と、前記ロックが解除された状態で所定の処理を行う処理手段と、前記処理が終了した後にロックを設定する第1のロック設定手段と、前記ロックが設定された後に前記フラグを解除するフラグ解除手段と、あらかじめフラグが設定されている場合に、ロックを設定する第2のロック設定手段とを有する。

【0032】この場合、ICカードにおいて、ロックを解除する前にフラグが必ず設定され、ロックが設定された後にフラグが解除されるとともに、あらかじめフラグが設定されている場合に、ロックが設定される。したがって、処理中にロックが解除された状態でICカードが奪取された場合、ICカードを不正に使用しようとしても、フラグがセットされているので、ICカードが自らロックを設定することになる。したがって、ICカードが不正に使用されることがなく、電子マネーが不正に引き出されることがない。

【図面の簡単な説明】

【図1】本発明の第1の実施の形態におけるICカードの支払処理方法を示すフローチャートである。

【図2】従来のICカードの取引処理方法を示すフローチャートである。

【図3】本発明の第1の実施の形態におけるICカードの支払処理装置を示すブロック図である。

【図4】本発明の第1の実施の形態におけるICカードの初期化動作を示すフローチャートである。

【図5】本発明の第2の実施の形態におけるICカードの支払処理方法を示す第1のフローチャートである。

【図6】本発明の第2の実施の形態におけるICカードの支払処理方法を示す第2のフローチャートである。

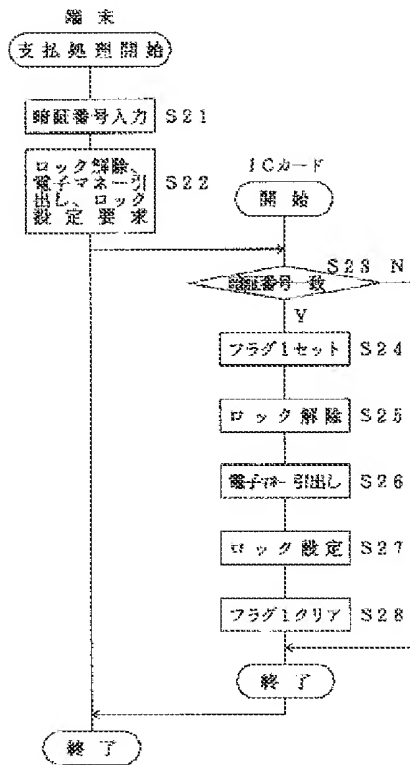
【符号の説明】

10 ICカード

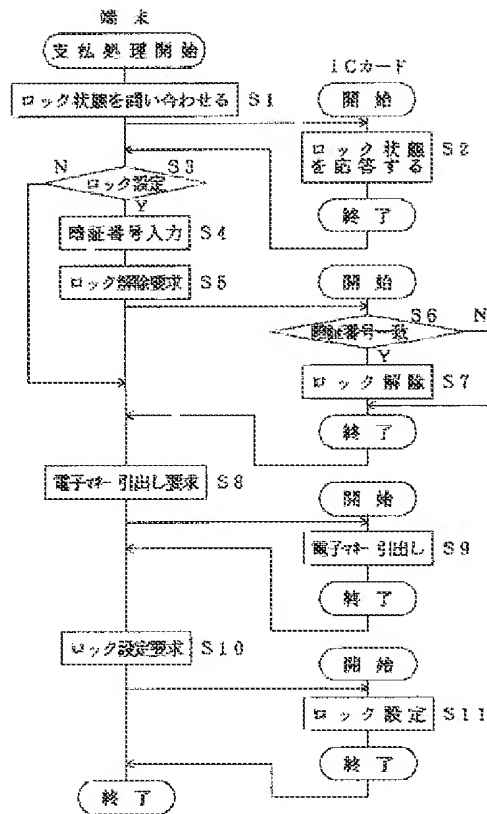
11 CPU

20 端末

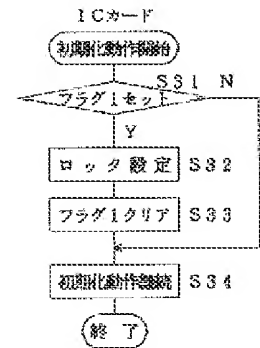
【図1】



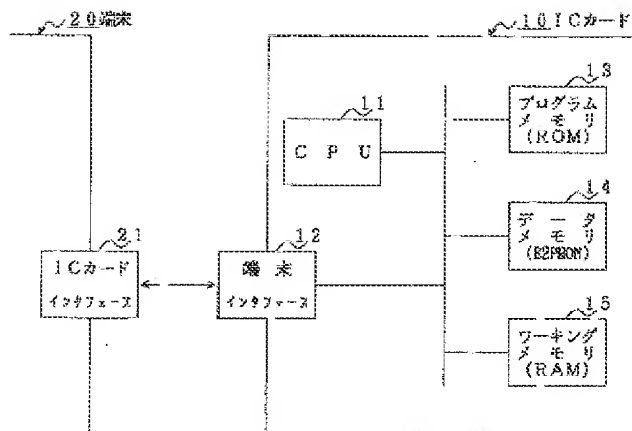
【図2】



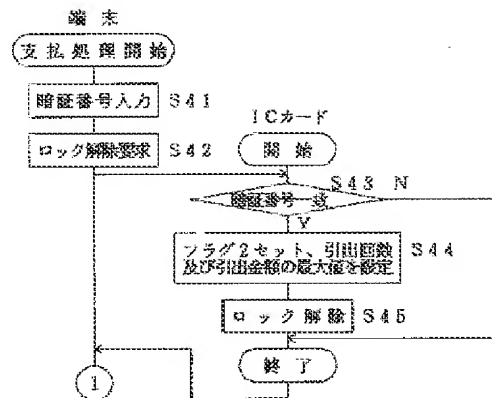
【図4】



【図3】



【図5】



【図6】

